CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI

June 12, 1996
Revision 0

LECTURE 14

LEDGE'S INTRODUCTION TO CRYPTARITHMS II

SUMMARY

It is my pleasure to present our guest lecturer LEDGE's (Dr. Gerhard D. Linz) second lecture on the interesting topic of Cryptarithms. In this lecture, he covers Multiplication, Multiplicative Structures, Base 11 and Base 12 calculations. LEDGE has a natural writing style, and a talent for making understandable some difficult concepts. LEDGE has already produced one of our better references on novice cryptography, and I appreciate his assistance in our course. Enjoy. [LEDG]

UNIQUE SOLUTION

Another Rule. Cryptarithms must meet another rule not stated in the first Lecture 8. There must be only one solution to the problem. That means that the solution must be unique.

For ease in reading we will now use "mod" for "modulo. See the previous cryptarithm lecture for the meaning of the term.

MULTIPLICATION

Let's start our analysis of reconstructing multiplication problems by looking at a typical multiplication of whole numbers as we learned it in grammar school:

```
  478
  x52
  ---
  956
2390
----
24856
```

For convenience in talking about this problem, we need to introduce some nomenclature. The number being multiplied, here 478, is called the "multiplicand." The number by which the multiplicand is multiplied, here 52, is the "multiplier."

The result of the multiplication, here 24856, is the "product."

If we analyze the parts or steps of this process, we find we have two separate multiplications and one addition in what we usually consider a single multiplication problem. The problem contains substeps: 2 x 478 = 956; 5 x 478 = 2390 and an addition to which we will turn in a moment. Notice in the second multiplication of the multiplicand by a digit in the multiplier, instead of 5 x 478 we really have 50 x 478. We don't write it that way because we moved the product of 5 x 478 one decimal place to the left and left a blank space for the product of 0 x 478 (which equals 0). If the multiplier had more digits, we would have continued to move the subsequent partial products another space to the left. We have done multiplications like this so often that we don't
usually recognize what we are doing.

Now we can look at the addition:

```
  956
 2390
-----
24856.
```

OBSERVATIONS

Each of these steps can give us different and valuable information.

1. The highest order digit of the multiplicand, multiplier, and product cannot be zero. In other words, by convention, no number starts with zero since no decimals are involved. If we had used letters in this example, the letters representing the 4 in 478, the 5 in 52, the 9 in 956, the 2 in 2390, and the 2 in 24856 could not represent 0.

2. The product of any sized multiplicand by a single digit multiplier can never contain more digits than the number of digits in the multiplicand plus one. If you need convincing, try it out with examples of your choice. In this case we have one such example: 5 x 478 = 2390. The multiplicand has three digits, the product four.

3. If a product has more digits than the multiplicand, the highest order digit of the product is less than or equal to the lower of the multiplier or the highest order digit of the multiplicand. Here, 5 x 478 = 2390. The highest order digit of the product is 2, smaller than the 4 of the multiplicand which in turn is smaller than the multiplier, 5.

4. The addition step is subject to the kinds of analyses we saw in the first lecture.

When solving multiplication cryptarithms, you may want to write out the separate parts of the problem as CROTALUS has suggested. In this lecture we will use the understandings we have developed, but leave the problem intact. [CROT]

The units digits of the products (the digit on the right end of each product) also can produce useful information which we will address later.

Example 1. Now let's tackle an example that should not be too difficult. This one is a C-6 from the March-April, 1995, issue of The Cryptogram by DYETI. The key is two words (9-0).

```
   LARK
   xCAR
  -----
  OOYRR
 ORLOA
LEECC
-------
LOSBRLR
```

SOLUTION OF EXAMPLE 1

By now you should be able to see the various parts of the problem: three multiplications of the multiplicand by R, A, and C; and the addition of the three partial products, each one after the first shifted an additional space to the left to give the final product, LOSBRLR.

Let's start with something familiar, the addition. We can notice that the leftmost digit of LEECC, the L, is carried to the final product without change; hence the sum of O and E, the next digits on the right, is less than 10 as there was no carry to the L. Finally, O + E + (0, 1 or 2) = O without a carry to the L. The (0, 1, or 2) are the possible carries from the previous addition of O + R + E plus a carry. But the only way for O + E = O mod 10 without a carry is for O + E = O not O + 10. As a result E = zero. Now let's take a look at the partial products. The products of C, A, and R times LARK is in no case LARK. Hence none of C, A, and R = 1. However, the product of R x K = R mod 10. The product of A x K = A mod 10, and the product of C times K = C mod 10.

There is only one value of K that would make that true. K must = 1. Furthermore, there is no carry in any of those multiplications.

That takes care of the information we can gather from the examination of the units digits.

With a carry of 0 from the first multiplications, we can look similarly at the result of multiplying each of the digits in the multiplier by the tens digit of the multiplicand, the R: R x R = R mod 10 (the tens digit in the first partial product). A x R = O mod 10 and C x R = C mod 10. Looking at the first product, R x R, the only digits that give themselves as the units number of their products when multiplied by themselves are 0 x 0 = 0; 1 x 1 = 1; 5 x 5 = 25 or 5 mod 10; and 6 x 6 = 36 or 6 mod 10. We already know what letters represent 0 and 1 so R = 5, or 6.

Both 5 and 6 are interesting numbers when considered from a multiplication standpoint.
5 x an even number = 0 mod 10. 5 x an odd number = 5 mod 10. Hence any product of 5 must end in either 5 or 0, two choices. Here we have three different products of R, not two. So R = 6.

Let's take a look at the products of 6 mod 10 since we have the product C x R = C: 6 x 2 = 2; 6 x 4 = 4, 6 x 8 = 8, all mod 10. The general rule is that R must be even for 6 x R = R. Furthermore, since R is even, the product of R x n is even for any digit value of n. The only way to get an odd numbered product is to multiply two odd numbers. Try it out. So C = 2, 4, or 8. Can we narrow that down? It turns out that we can.

Each of the partial products is 5 digits long, one more than the multiplicand. From fact 3 above, we know that the highest order digit in each case cannot be larger than the lower of the single digit multiplier and the highest order digit of the multiplicand. The highest order digits of the partial products are O, O, and L. Since L is the highest order digit of the multiplicand, C x LARK must yield the largest product. The highest possible value of C is 8. The next one is 4. Almost certainly C = 8.

Let's put our number-letter equivalents into a table:

```
9 8 7 6 5 4 3 2 1 0
  C   R         K E.
```

We're supposed to find two words at the end of this process. The letters we have make a promising beginning.

The product C x LARK = LEECC or, since we know many of the values of the letters, 8 x LA61 = L0088. Let's go through that multiplication step by step. 8 x 1 = 8, no carry. 8 x 6 = 48, carry the 4. 8 x A + 4 (the carry) must = 0 mod 10; so 8 x A must = 6 mod 10 since 6 + 4 = 0 mod 10. The products of 8 that end in 6 are 16 and 56; so A = 2 or 7. The addition section will give us the clue we need.

At the tens digit of the addition R + A = L mod 10. We know R is 6. If A = 2, then R + A = 8, not possible since C = 8 already. So A = 7. R + A = 6 + 7 = 3 mod 10 or L = 3. Dividing the product LEECC or 30088 by 8 (C) gives 3761 for LARK. O could = 1 or 2, but only 2 is available (why?). Multiplying LARK x R will give us Y in the first partial product = 5. Only B has not been determined. By default it must be = 4. The key tableau is 9 8 7 6 5 4 3 2 1 0.

S C A R Y B L O K E

The final result :

```
   3761
   x876
  -----
  22566
 26327
30088
-------
3294636
```

Example 2. Let's try another. If you feel brave, try it on your own before reading the explanation. It's not any more difficult than the first problem, only different.

On the third page of Lecture I we presented this multiplication problem by APEX DX:

```
 OTTAWA
    xON
 ------
HNNTLIL
IIIEHE
-------
TOOINRL
```

SOLUTION OF EXAMPLE 2

In Lecture 8, we determined that the only candidates for the representation of zero were L, W and R. We carried the solution no further at that point. We can do better than that with the tools we now have.

The problem contains two partial products, N x OTTAWA = HNNTLIL and O x OTTAWA = IIIEHE, plus the addition of those products to give the final product. TOOINRL. We now note that the second partial product and the multiplicand have the same number of digits, six.

Further, the highest order digit of the multiplicand and multiplier are the same, namely O. O x O + carry = I. The highest digit O can represent is 3 as 3 x 3 = 9. Any higher digit when multiplied by itself gives a two-digit result, adding a digit to that partial product. If O = 3, then I = 9. The partial product become 999EHE. Dividing by the multiplier value, 3 produces 333??? for OTTAWA. That cannot be since we have only one digit per letter. O also is not one, for multiplying any number by one results in that number. Therefore O must be = 2. 2 x 2 = 4 and the partial product would 444EHE. Again, dividing by 2 give 222???. As before I cannot equal T. Since 2 x 3 is 6 and I is less than that, I = 5, and the partial product is 555EHE. Dividing by O or 2, the multiplier, gives 277??? for OTTAWA; hence T = 7. In lecture I we were left with L, W, and R as the only possible candidate for the digit, 0. At that time we could not unambiguously select one of these as representing zero. We can now eliminate L from consideration. Look at the problem to see if you can spot how.

L comes from the product of N x A mod 10. For L to be = zero, either N or A must be = 5. We have already determined that I = 5. Neither N or A are five, so L cannot be zero. We are left to choose between R and W.

Our letter-number equivalent table now is:

```
0 1 2 3 4 5 6 7 8 9
  O     I   T
```

At the moment we can make no progress with the second partial product so let's examine the first, N x OTTAWA = HNNTLIL. Substituting the identified digits we have N x 277AWA = HNN7L5L. This product has seven digits, one more than OTTAWA. We have learned that the highest order digit of such a product must be less than or equal to the lower of the multiplier or the highest order digit of the multiplicand, i.e, O or N. Since O = 2, H can only = 1. We add that to the letter-number equivalent table. The partial product becomes N x 277AWA = 1NN7L5L. Dividing the product by OTTAWA or 277AWA, we learn that N could be 4,5, or 6. Since I = 5, N must be 4 or 6.

Still working with the first partial product, N x A = L mod 10. A is multiplied by N again when we reach the hundreds digit of OTTAWA. Again the result is L mod 10. How could this be? It can only happen if there is no carry from the product of N x W. In the second partial product 2 x A = E mod 10 two times, as before. Thus 2 x W cannot have a carry here as well. Neither 4 x W, 6 x W, nor 2 x W > 9. W can only be 0 or 1. Because H = 1, W = 0.

We could have gone another route. In the addition I + E = R. If R were = 0, since I = 5, E would have to be 5 also. That's not allowed, so R cannot be 0 and only W is left to = zero. Still a third way of determining whether R or W = zero is by anagraming. If R = zero, we look at the equivalent table and the keyword would have to start RHO, not impossible, but not encouraging. If W = zero, the keyword starts WHO, a word, very encouraging. Just like in K1 and K2 Aristocrats, reconstructing the equivalent table (instead of the equivalent alphabets) can give us useful clues. I generally use anagraming only as a last resort if I am otherwise stymied, however.

With W = 0 we know that O x A = HE and N x A = IL. Replacing known letter values, we have 2 x A = 1E and N x A = 5L. The only products in the 50's produced by multiplying two single digit numbers are 54 and 56 or 9 x 6 or 7 x 8. Since

T = 7, we cannot use N = 7 to yield N x A = 56; hence N and A are 9 and 6 and L = 4. We know that N is 4 or 6 (see above). So N = 6, A = 9, and, since 2 x 9 = 18, E = 8. The results are consistent; they produce no redundancies.

The equivalent table becomes:

```
0 1 2 3 4 5 6 7 8 9
W H O   L I N T E A.
```

Only the R needs to be placed. What are the three words? Whorl in tea (Tempest in a teapot???).

PROBLEMS IN BASES OTHER THAN TEN

Our number system is based on the number 10, perhaps because normally humans have ten fingers and ten toes. So having ten for a base makes counting easier. We generally write our numbers as a series of digits with or without a decimal point, but we read the real value of a digit by its position in relation to the decimal point, either provided or tacitly understood. So we read 5,678 as five thousand, six hundred, seventy eight. Translating the English into number it becomes 5 x 1000 + 6 x100 + 7 x 10 + 8 x 1. That process is pure convention, but we don't usually think about it.

Notice also that we have ten different characters for the ten different digits. When we count from zero up in whole numbers we use all ten (0-9) to get to 9 and then we move on to two digits, using a one in the tens place and starting anew with zero in the units place. It takes a lot of words to explain it, but we're so used it; we just spout the number and go on.

Yet it is pure convention that we use ten as the base. We call it decimal, using the Greek word for ten. In fact we could use any whole number as the base except, of course, 0 alone as we can't count with it. Whatever number we use as a base, that's how many characters we need. If we were to want to count base 2 (like a series of switches that are either on or off), we'd need only the digits 0 and 1. That's called the binary system. Counting would go as follows:

```
Base 2:  0 1 10 11 100 101 110 111 1000 1001 1010 1011 1100 1101
Base 10: 0 1  2  3   4   5   6   7    8    9   10   11   12   13
```

Notice that in binary 1101 = 1 x 8 + 1 x 4 + 0 x 2 + 1.
In decimal we would read as 1 x 1000 + 1 x 100 + 0 x 10 + 1 x 1.

Just as 1000 is 10x10x10, so 8 is 2 x 2 x 2. 100 is 10x10; 4 is 2 x 2. Binary 1000 translates to decimal 8, etc. Binary 1101 = Decimal 13. Naturally with only two symbols, binary representation of numbers are much longer than base 10 representations.

We used base two as an illustration only. Cryptarithms, if not in decimal or base 10 form, use bases that are larger than ten, most often 11, called undecimal, or 12, called duodecimal. For undecimal we need to create a new character to replace decimal 10. Usually, "x" is used. Since we are using x as the multiplication symbol, we will use "t" for ten. We need another symbol for decimal 11. Usually, "e" is used.

Counting in undecimal goes like this: 1, 2, 3, 4, 5, 6, 7, 8, 9, t, 10, 11, 12 etc. What we are used to reading as 10 is really 11 base 10. 11 is really 12 base 10, etc. In duodecimal counting proceeds 1, 2, 3, 4, 5, 6, 7, 8, 9, t, e, 10, 11, 12, etc. Looks are deceiving and you have to be careful. What looks like ten is read as 12, 11 is really decimal 13. If you have a number like 378 in duodecimal, think 3 x 12 x 12 + 7 x 12 + 8 or 3 x 144 + 7 x 12 + 8. If you wish, you can think three hundred seventy eight, but you must remember that in our ordinary notation 100 base 12 = 144 base 10 and 10 base 12 = 12 base 10. Arithmetical problems are solved as always, taking note of the different notation.

If you find the following explanations which involve arithmetical manipulations in base 11 and 12 confusing, consult the multiplication and addition tables in the Appendix. [Tables 14-1 - 14-4]

DUODECIMAL

Now let's look at some duodecimal examples.

Example 1. Addition

```
 497
+876
----
1151.
```

It looks odd, but it's duodecimal. 7 + 6 = 13. Divide by 12 and you get a quotient of 1 and a remainder of 1. Put down the remainder and carry the quotient of 1. 9 + 7 + 1 (carry) = 17. Divide by 12 giving a quotient of 1 and a remainder of 5. Put down the remainder of 5 and carry the quotient of 1. 8 + 4 + 1 (carry) = 13. Divide by 12 giving a quotient of 1 and a remainder of 1. Put down the remainder of 1 and, because the next column adds to 0 + 1 (the carried quotient), put down another 1. If we had an addition of 4 + 6 = ten, we would not divide by twelve but merely put down the ten as t. So in duodecimal 4 + 6 = t.

Example 2. Subtraction.

```
 67
-39
 --
 2t.
```

To subtract 9 from 7 we must borrow 12 from 6, making it 5. 12 + 7 - 9 = 10 or t. We put that down. 6 - 1(borrow) - 3 = 2. Hence the answer is 2t.

Example 3. Multiplication.

```
  67
 x39
 ---
 4e3
179
----
2083
```

The process in words: 9 x 7 = 63, divide by 12 giving quotient of 5 and remainder of 3. Put down the 3 and carry the quotient of 5, just as in addition. 9 x 6 + 5(carry) = 59. Divide by 12 giving 4 as quotient and 11 or e as the remainder. Put down the remainder of e and, since there are no more digits to multiply by 9, put down the quotient of 4. Let's check this last one: 4 x 12 + 11 = 48 + 11 = 59. Work through the rest of this example on your own.

Example 4. Division.

```
    2e
   ---
17/48t
   32
   --
   16t
   155
   ---
    15
```

First, we choose a trial quotient, here 2, and multiply the divisor, here 17, by it. 2 x 7 is 14, divide by 12 getting a remainder of 2 and a quotient of 1. Put down the 2 and carry the 1. 2 x 1 + 1(carry) = 3. Put it down. Bring down the next digit of the dividend, here t. Now go on your own and check out my work.

Undecimal works the same way, except that instead of dividing by 12, we would divide by 11. If all that dividing and translating is too much to remember, use the proper multiplication table in the Appendix. Just as in the base 10 or decimal multiplication table the product of one digit by another is a one-digit or a two digit number, so it is in undecimal and duodecimal. In fact that's true of any base greater than 2. Be careful about reading and manipulating an undecimal or duodecimal number as a decimal number. The occasional t and e will remind you, but it's easy to forget momentarily, even after you've been at it for a while.

MULTIPLICATIVE STRUCTURES

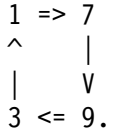
FIRE-O in the May-June, 1970, issue of The Cryptogram introduced the concept of multiplicative structures [FIRE-O]. In 1977, in a two part article on base 11 and 12 arithmetic, I expanded on FIRE-O's work by extending the multiplicative structures to the higher bases [LEDG1] and [LEDG2]. The concept is simple, but often very useful. [FIRE]

Let's take a digit, like 7, multiply it by 1 and then multiply it successively by the resulting product, i.e., when we multiply again we use the latest product. All the multiplications will be mod 10 as we are only interested in the units digit of the product. With using 7 we get:

1 x 7 = 7 7 x 7 = 9 9 x 7 = 3 3 x 7 = 1

Notice that the last product in the series in this case results in the multiplier we started with, 1. For 7 we have found a circular structure: (= 1 => 7 => 9 => 3 =). I am using the symbols =) and (= as indicators to return to the other end of the series.

We could also diagram it as:



You can read the series as 1 to 7 to 9 to 3 to 1 to 7 etc.

Because of the lack of printable characters in ASCII, I'll be using the first kind of diagram. Notice that all the digits in the diagram are odd. We can start another diagram by starting with an even number, say 2.

2 x 7 = 4 4 x 7 = 8 8 x 7 = 6 6 x 7 = 2 or

(= 2 => 4 => 8 => 6 =).

That leaves 5 x 7 = 5 or 5 <=, and 0 x 7 = 0 or 0 <=. In other words, multiplying 7 by 5 or 0 gives the multiplier as the units digit of the product. The last is true for any odd number.

As we will see shortly, 3 diagrams out in a similar fashion to 7, two circles, one of odd numbers and one of even ones.

If n is odd, then 5 x n => 5. Diagram: 5 <=.
If n is even, then 5 x n => 0. Diagram 5 => 0 <=
In both cases, 0 x n => 0 and 0 x 0 => 0. Diagram 0 <=.

Now let's look at the other diagrams.

BASE 10.

```
0: n x 0 <=

1: n x 1 => n <=. In other words, successive multiplications by  1 always yield n.

2:    1    7    9    3   2 X 2 = 4   4 X 2 = 8 etc.
      |    |    |    |   1 x 2 = 2   7 x 2 = 4 etc.
      V    V    V    V   and 5 => 0 <=.
   (= 2 => 4 => 8 => 6 =)

3. (= 1 => 3 => 9 => 7 =)    5 <=  and 0 <=
   (= 2 => 6 => 8 => 4 =)

4. 1 => 4 <==> 6 <= 9;   3 => 2 <==> 8 <= 7;  5 => 0 <=

5. odd x 5 <=;  even x 5 => 0 <=

6. 1 => 6 <=;  3 => 8 <=;  5 => 0 <=;  7 => 2 <=; 9 => 4 <=.

7. (= 1 => 7 => 9 => 3 =)      5 <=  and 0 <=
   (= 2 => 4 => 8 => 6 =)

8.    1    3    9    7     5 => 0 <=
      |    |    |    |
      V    V    V    V
   (= 8 => 4 => 2 => 6 =)

9. 1 <==> 9; 2 <==> 8;  3 <==> 7;  4 <==> 6   5<=   0 <=.
```

Remember that in each case, each resulting product (mod 10) is multiplied by the original multiplier given at the beginning of each set, e.g., " 6.".

BASE 11 (UNDECIMAL)

```
0. n x 0 => 0 <=

1. n x 1 => n <=

2. (= 1 => 2 => 4 => 8 => 5 => t => 9 => 7 => 3 => 6 =)   0   <=

3. (= 1 => 3 => 9 => 5 => 4 =); (= 2 => 6 => 7 => t => 8 =); 0 <=

4. (= 1 => 4 => 5 => 9 => 3 =); (= 2 => 8 => t => 7 => 6 =); 0 <=

5. (= 1 => 5 => 3 => 4 => 9 = ; (= 2 => t => 6 => 8 => 7 =); 0 <=

6. (= 1 => 6 => 3 => 7 => 9 => t => 5 => 8 => 4 => 2=); 0 <=

7. (= 1 => 7 => 5 => 2 => 3 => t => 4 => 6 => 9 => 8 =); 0 <=

8. (= 1 => 8 => 9 => 6 => 4 => t => 3 => 2 => 5 => 7 =); 0 <=

9. (= 1 => 9 => 4 => 3 => 5 =); (= 2 => 7 => 8 => 6 => t =); 0 <=

t. 1 <==> t; 2 <==> 9; 3 <==> 8; 4 <==> 7; 5 <==> 6;  0 <=
```

BASE 12 (DUODECIMAL)

0. n x 0 => 0 <=

1. n x 1 => n <=

2. 1,7 => 2 => 4 (==> 8 <= t <= 5,e; 3,9 => 6 => 0 <=

3. 1,5 => 3 <==> 9 <= 7,e; 2,t => 6 <=; 4,8 => 0 <=

4. 1,7,t => 4 <=; 2,5,e => 8 <=; 3,6,9 => 0 <=

5. 1 <==> 5; 2 <==> t; 4 <==> 8; 7 <==> e; 3,6,9 0 <=

6. 1,3,5,7,9,e, => 6 => 0 <= 0,2,4,8,t

7. 1 <==> 7; 3 <==> 9; 5 <==> e; 0 <=; 2<=; 4 <=; 6 <=; 8 <=; t <=;

8. 1,7,t => 8 <==> 4 <= 2,5,e; 3,6,9 => 0 <=

9. 1,5 => 9 <=; 2,7 => 6 <=; 7,e => 3 <=; 4,8 => 0 <=;

t. 1,7 => t => 4 <=; 5,e => 2 => 8 <=; 3,9 => 6 => 0 <=;

e 1 <==> e; 2 <==> t; 3 <==> 9; 4 <==> 8; 5 <==> 7; 6 <=; 0 <=

Notes:
1) In each system 1 x n = n and 0 x n = 0.

2) In each system the two digits involved in each structure for the highest digit (base - 1) add up to the base. Another way to look at that is to realize that the digits in the product of n x (base - 1) add up to base - 1. Thus, in decimal 8 x 9 = 72 and 7 + 2 = 9 (10 - 1). In undecimal, 6 x t = 55 and 5 + 5 = t. Finally, in duodecimal, 9 x e = 83 and 8 + 3 = e.
3) The structure for 5 (which = base/2) in decimal has the same form as for 6 (which also = base/2) in duodecimal. Undecimal, being odd, has no equivalent for 5 and six.

DUODECIMAL MULTIPLICATION EXAMPLE

To begin to put some of these findings together, let's tackle a duodecimal multiplication example. In the process we will discover the usefulness of the multiplicative structures for at least some of the more difficult or complicated multiplication problems and, by extension, division problems as well. You remember that division problems have one or more partial multiplications in them.

Here's the problem: It's by MORDASHKA and appeared as C-11 in the November-December, 1994, issue of The Cryptogram.

```
    YOUR
     TAB
    ----
   IYATR
  UOYLN
 PYPRR
-------
YCROTR
```

The problem contains three partial products and one addition with three addends shifted as per usual for multiplication. It could be helpful if we can locate zero. We could use a process of elimination. Neither Y, T, A, B, I, U, P, nor R can be zero. That leaves four letters as possibilities: C, O, N, and L. Fortunately for us, in the addition section we find T + N = T. Hence N = zero.

Also from the addition section at the left end, Y > P. U + Y must be greater than e, giving a carry of 1, so Y = P + 1. That should be useful later.

Again from the addition section, A + L + R = R mod 12. There is no carry from the previous column: T + N as N = 0. We can subtract R from both sides of the first equation giving us A + L = 0 mod 12. But A and L are both greater than 0 so A + L = 10 or decimal 12. That means if we can determine the value of A, we can compute the value of L from the equation, and vice versa.

>From the partial products, all of which are 5 digits long whereas the multiplicand is 4 digits long, Y > I, U, P > 0. Therefore Y must more than 3. Now let's look at the partial products to see whether we can uncover a recognizable multiplicative structure, remembering that we are dealing with a duodecimal or base 12 problem. We get these equations from the product of the last digit of the multiplicand by each digit of the multiplier:

R x B = R R x A = N or zero R x T = R all mod 12

The multiplicative structure becomes: B,T => R and A => zero.

There are only two places that yield the appropriate relations, when R = 4 or R = 8. Since none of R, B, and T equal 1 and R does not equal zero, here are the results:

R = 4 then B and T are 7 and t or t and 7. A = 3, 6, or 9.
R = 8 then B and T are two of 7, t, and 4. A = 3, 6, or 9.

That's not very many possibilities, simplifying our search. The first partial product ends with TR. The third ends with RR. If we identify T and B, we should be able to calculate U in the multiplicand and check it in both partial multiplications.

So here's our table:

B	T	R	U
7	t	4	
t	7	4	
7	t	8	
t	7	8	
4	t	8	
t	4	8	

Those are the only possible values of B, T, and R, all the permutations. In each instance we have to calculate U to discover what value of U is consistent in both multiplications.

Now let's check these possibilities. B x YOUR = IYATR.

1) B = 7, T = t, R = 4, TR = t4. B x R = 7 x 4 = 28 base 10 or 24 base 12. Carry the 2. B x U + 2 => T or t. 7 x U + 2 => 4, U = 8. Check: 7 x 8 + 2 = 58 base 10 or 4t base 12 or t mod 12. Our trial value for U is 8. Let's check that with the third partial product T x YOUR = PYPRR. T = t etc. as before. RR = 44. t x 4 = 40 base 10 or 34 base 12. Carry the 3. t x 8 + 3 = 83 base 10 or 6e base 12 or e mod 12, but we needed a 4 for 44. It doesn't work.

2) We have to continue the process until we get a combination that is consistent. Try the second one. You may find that no value of U can be found from the first partial. Similar problems beset the next three combinations on the table.

3) Let's check the 5th combination. B = 4, T = t, R = 8, TR = t8. B x R = 4 x 8 = 32 base 10 or 28 base 12 or 8 mod 12. Carry the 2. B x U + 2 = t mod 12. 4 x U + 2 = t. U could be 2 or 5. Try them with the second product. RR = 88. T or t x 8 = 80 base 10 or 68 base 12 or 8 mod 12. Carry 6. For U = 2, t x 2 + 6 = 26 base 10 or 22 base 12 or 2 mod 12. But we need an 8 for 88. That's a conflict. Let's try U = 5. t x 5 + 6 = 56 base 10 or 48 base 12 or 8 mod 12. Eureka! U = 5 checks out. We now also know that B = 4, T = t and R = 8. You can check the last combination also to make sure it produces no alternate value of U that stays consistent.

The letter-number equivalent table is

```
0  e  t  9  8  7  6  5  4  3  2  1
N     T     R        U  B
```

We can now determine the value of A using fact 4) A + L = 12 with the middle partial product. A x YOUR = UOYLN or A x ..58 = (12 - A)0. A can have the value of 3, 6 or 9. If A is 6, then L = 6 (A + L = 12, remember?). That's not possible. If A = 3 L = 9. If A = 9, L = 3. Try 3. 3 x 8 = 24 base 10 or 20 base 12. Carry the 2. 3 x 5 + 2 = 17 base 10 or 15 base 12 or 5 mod 12. But we needed a 9. Try A = 9. It better work or we've done something wrong. 9 x 8 = 72 base 10 or 60 base 12. Carry the 6. 9 x 5 + 6 = 51 base 10 or 43 base 12 or 3 mod 12. So L = 3. That's the value of L we were looking for. Success! We can add that to the equivalent table. With A = 9 and T = t, T x YOUR = A x YOUR + YOUR.

Since we know that T x YOUR = PYPRR and A x YOUR = UOYLN, we can put the addition into normal form:

```
 UOYLN
 +YOUR
 -----
 PYPRR
```

>From this addition we deduce that P = U + 1 or 5 + 1 = 6.

Looking at the multiplier, TAB = t93. The first product must be the smallest, followed by the second, with the third the largest. Their leftmost digits must be in the same order. Hence, I < U < P < Y.or Y > P > U > I. The only letters about which we have no information yet are C and O.

At this point our equivalent table reads:

```
0  e  t  9  8  7  6  5  4  3  2  1
N     T  A  R        U  B  L
```

Replacing letters of known value in the above addition by their respective digits yields

```
 50Y30
 +Y058
 -----
 PYP88
```

We note that Y + O = P and O + Y = Y. 3 + 5 = 8, no carry. Y + O must yield a carry of 1 which makes Y = P + 1. Since I < U, the only place in the table for two numbers that are adjacent in value is 7 and 6; thus Y = 7 and P = 6. Y + O = P mod 12. That means 7 + O = 16 base 12 or 18 base 10. Thus, O = e. The addition of all three partial products will give us the remaining values for I and C without resorting to anagraming. (Just a nicety here.)

```
   I79t8
  5e730
+67688
--------
 7C8et8
```

9 + 3 + 8 = 18 base 12. Carry 1. 7 + 7 + 8 + 1 = 1e base 12. Carry 1. I + e + 6 + 1 = 8 or 18 base 12. Solving for I gives I = 2. Carry 1. 5 + 7 + 1 = 11 base 12. Thus C = 1. The keyphrase for the equivalent table becomes NOTARYPUBLIC.

Although this problem was given the number C-11, for someone familiar with duodecimal arithmetic it is of medium difficulty. There are problems in the Cryptarithm section that provide far fewer clues and necessitate trying out many more possibilities. In the next lecture we will take a look at organizing that process so as not to get lost in the bookkeeping aspect of finding a solution. We may also find a few more relationships that can be helpful at times.

REFERENCES

[CROT] Winter, Jack (CROTALUS), "Solving Cryptarithms," American Cryptogram Association, 1984.

[FIDD] FIDDLE, Lynch, Frederick D., "An Approach to Cryptarithms," ACA Publications, 1974.

[FIRE] FIRE-O, "A Tool for Mathematicians: Multiplicative Structures," The Cryptogram, Volume XXXVI, No 3, 1970.

[LED1] LEDGE, "Basic Patterns in Base Eleven and Twelve Arithmetic (Part 1)," The Cryptogram, Volume XLIII, No 5, 1977.

[LED2] LEDGE, "Basic Patterns in Base Eleven and Twelve Arithmetic (Part 2)," The Cryptogram, Volume XLIII, No 6, 1977.

APPENDIX

Table 14-1

Undecimal Multiplication Table

	1	2	3	4	5	6	7	8	9	t
1	1	2	3	4	5	6	7	8	9	t
2	2	4	6	8	t	11	13	15	17	19
3	3	6	9	11	14	17	1t	22	25	28
4	4	8	11	15	19	22	26	2t	33	37
5	5	t	14	19	23	28	32	37	41	46
6	6	11	17	22	28	33	39	44	4t	55
7	7	13	1x	26	32	39	45	51	58	64
8	8	15	22	2x	37	44	51	59	66	73
9	9	18	25	33	41	4t	58	66	74	82
t	t	19	28	37	46	55	64	73	82	91

Table 14-2

Duodecimal Multiplication Table

	1	2	3	4	5	6	7	8	9	t	e
1	1	2	3	4	5	6	7	8	9	t	e
2	2	4	6	8	t	10	12	14	16	18	1t
3	3	6	9	10	13	16	19	20	23	26	29
4	4	8	10	14	18	20	24	28	30	34	38
5	5	t	13	18	21	26	2e	34	39	42	47
6	6	10	16	20	26	30	36	40	42	50	56
7	7	12	19	24	2e	36	41	48	53	5x	65
8	8	14	20	38	34	40	48	54	60	68	74
9	0	16	23	30	39	46	53	60	69	76	83
t	t	18	26	34	42	50	5x	68	76	84	92
e	e	1t	29	38	47	56	65	74	83	92	t1

Table 14-3

Undecimal Addition Table

	1	2	3	4	5	6	7	8	9	t
1	2	3	4	5	6	7	8	9	t	10
2	3	4	5	6	7	8	9	t	10	11
3	4	5	6	7	8	9	t	10	11	12
4	5	6	7	8	9	t	10	11	12	13
5	6	7	8	9	t	10	11	12	13	14
6	7	8	9	t	10	11	12	13	14	15
7	8	9	t	10	11	12	13	14	15	16
8	9	t	10	11	12	13	14	15	16	17
9	t	10	11	12	13	14	15	16	17	18
t	10	11	12	13	14	15	16	17	18	19

Table 14-4

Duodecimal Addition Table

	1	2	3	4	5	6	7	8	9	t	e
1	2	3	4	5	6	7	8	9	t	e	10
2	3	4	5	6	7	8	9	t	e	10	11
3	4	5	6	7	8	9	t	e	10	11	12
4	5	6	7	8	9	t	e	10	11	12	13
5	6	7	8	9	t	e	10	11	12	13	14
6	7	8	9	t	e	10	11	12	13	14	15
7	8	9	t	e	10	11	12	13	14	15	16
8	9	t	e	10	11	12	13	14	15	16	17
9	t	e	10	11	12	13	14	15	16	17	18
t	e	10	11	12	13	14	15	16	17	18	19
e	10	11	12	13	14	15	16	17	18	19	1t

LECTURE 13 SOLUTIONS

13-1 Beaufort

```
ABRVJ  UTAMP  YPLHZ  OZYAP  YPJNP  KNXUG
QRDPC  ELPNC  BVCEF  NLLSJ  LGOWC  VYCGA
EVGIX  XNDKY  U.  (butter) (INWVQH)
```

Key = AGRICULTURE, A fantastic glut ...

13-2 Vigenere.

```
DWNIT  KGEWZ  ENJQZ  WXLLZ  WZOKC  ETOWI  NXVQS
DQGAK  MGGBH  NAMWE  OWVAM  UJDVQ  IMDSB  VCCTR
YUIQX.  (making, UHVW)
```

Key = LIBERTY, Some criminals in ....

13-3 Vigenere Running Key

```
YPOSC  DWVWY  CCHZT  AKALF  I.  (tolls -2)
```

Key = Never send for whom the be (continues bell tolls)

13-4 Vigenere Progressive key. "Fungi"

```
IPGPUPX  GTIAKNP  AMEHLAW  SJSTROZ  TCGYUND  STNPJZM
OESWAXG  VLHSPZC  GNEIWHP  EKHNOWW  PMEQFVV  PDQAWCA
GGFRKSO  RCHZVKL  NBWHYBV  CUNBBBB  AVGCJFA  FLTMKUV  K.
```

Key = PICTURE (3), The way to identify....

LECTURE 14 PROBLEMS

Some time ago, CROTALUS cooked up some goodies:

14-1. Multiplication (Two words, 0-1) original by EDNASANDE

WOMEN X MEN = UTNNLM + NWTWNN = NLSMTUWM

14-2. Division (Two words, 0 -9) MORDASHKA

ATOM / ASK = N; - GNC = IS

14-3. Multiplication. (No word, 0-1) FOMALHAUT

ASAP X MAB = RITMT + TMPRY + PDBYD =PAYDIRT

14-4. Unidecimal multiplication. (Two words 0-X) WALRUS

TOUGH X DIG = IDIGDN + NYYDNG + UIHDOU = DDCUUILN